PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Central Index of Investigations (DCII)
Defense Manpower Data Center

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 6697
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes**
- ☐ **No**

If "Yes," enter UPI 2865

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DMDC 11 DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. in progress

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ **Yes**

Enter OMB Control Number	in progress
Enter Expiration Date	in progress

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 301, Departmental Regulations; E.O. 10450, Security Requirements for Government Employment; DoD Directive 5200.2, DoD Personnel Security Program (32 CFR part 156); and E.O. 9397, as amended (SSN)

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

DCII is an automated central repository that identifies investigations conducted by DoD investigative agencies. The DCII database consists of an index of personal names and titles that appear as subjects, victims, or cross-referenced incidental subjects, in investigative documents/files maintained by DoD criminal, counterintelligence, fraud, and personnel security investigative activities.
Types of personal information collected include: names, other known alias, SSN, date of birth, state of birth, country of birth.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Access to personal information is limited to those individuals who manage the records, make adjudication determinations, or perform other official duties. Activities must be a part of DoD/Federal Government and accredited on the basis of authorized requirements. Access to personal information is restricted by the use of passwords which are changed periodically. All data transfers and information retrievals that use remote communication facilities are encrypted. Electronic records are maintained in encrypted database in a controlled area accessible only to authorized personnel. Entry to these areas is restricted by the use of locks, guards, and administrative procedures.

As of February 2005, DCII does not actively index files pertaining to clearance investigations. If an indexed file associated with a clearance investigation is discovered, it should be removed.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. PERSEREC, DLA

☒ **Other DoD Components.**

Specify. USA, USAF, USMC, NAVY, NSA, DSS, DIA

☒ **Other Federal Agencies.**

Specify. FBI, OPM, SIGIR, USAID, USCG

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. SAIC: Protection of Personally Identifiable Information (PII)
(a) To the extent that the work under this task order / agreement requires the contractor to have access to personally identifiable information about an individual (hereinafter referred to as "PII"), the contractor shall after receipt thereof, treat such PII as confidential and safeguard such information from unauthorized use and disclosure. The contractor agrees not to appropriate such PII for its own use or to disclose such information to third parties unless specifically authorized by the

Government, in writing.
(b) The contractor agrees to allow access only to those employees who need the PII to perform services under this task order and agrees that PII will be used solely for the purpose of performing services under this task order. The contractor shall ensure that its employees will not discuss, divulge or disclose any such PII to any person or entity except those persons within the contractor's organization directly concerned with the performance of the task order.
(c) Contractor shall administer a monitoring process to ensure compliance with the provisions of this clause. Any discrepancies or issues should be discussed immediately with the Contracting Officer Technical Representative (COTR) and corrective actions will be implemented immediately.
(d) The contractor shall report immediately to the DMDC CIO / Privacy Office and secondly to the COTR discovery of any Privacy breach. Protected PII is an individual's first name or first initial and last name in combination with any one or more of the following data elements including, but not limited to: social security number; biometrics; date and place of birth; mother's maiden name; criminal, medical and financial records; educational transcripts, etc.
(e) The Government may terminate this task order for default if contractor or an employee of the contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this task order, including criminal and civil penalties.
(f) In accordance with the Privacy Act of 1974 Section (m) (1) contractors supporting a Government agency shall be considered to be an employee of that agency. As such all contractors will be required to take Privacy training, provided by the Government, upon hiring and annually. Additional specialized training may also be required.
(g) The Contractor shall include this section in all appropriate subcontracts.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

Records are entered into DCII to identify investigations conducted by DoD investigative agencies. For criminal investigations, individuals do not have the opportunity to object to the collection of their PII. For clearance investigations potentially still in DCII, information provided by individuals for a security clearance was voluntary. Without voluntary disclosure of information on an SF86 (or a preceding form) an investigation cannot be completed in a timely manner and could negatively affect an individuals placement or security clearance prospects. If an individual objected to sharing the required personal information needed to initiate a security clearance then the individuals clearance request could not be processed.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Records are entered into DCII by DoD investigative agencies reflecting the existence of an investigation in progress. For criminal investigations, individuals do not have the opportunity to consent to the use of their PII. For clearance investigations potentially still in DCII, the SF86 EPSQ (or preceding form) was used to initiate or reinvestigate a persons eligibility for security clearance access. The SF86 EPSQ provides a list of Privacy Act Routine Uses under which a subjects information may be accessed by other than the person who is the subject of the SF86 EPSQ. When a subject signs and submits their SF86 EPSQ they consent to those Privacy Act Routine Uses.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ **Privacy Act Statement** ☒ **Privacy Advisory**

☐ **Other** ☒ **None**

Describe each applicable format.

For clearance investigations potentially in DCII:
Collection, maintenance, and disclosure of background investigative information is governed by the Privacy Act. These Privacy Act applications are acknowledged by the individuals signature on their SF86 EPSQ and in interviews between the individual and their clearance investigator.

For criminal investigations: NONE.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.